[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610076225.0

[43] 公开日 2007 年 10 月 10 日

[11] 公开号 CN 101052034A

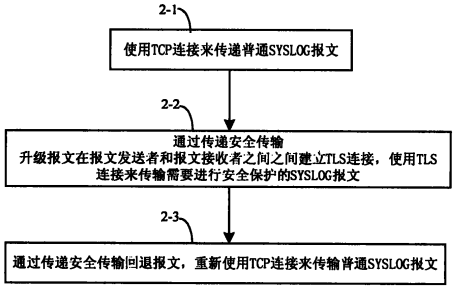
[22] 申请日 2006.4.19
[21] 申请号 200610076225.0
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 苗福友
[74] 专利代理机构 北京凯特来知识产权代理有限公司
代理人 郑立明
权利要求书 3 页 说明书 10 页 附图 2 页

[54] 发明名称

传输网络事件日志协议报文的方法和系统

[57] 摘要

本发明提供了一种传输网络事件日志协议报文的方法和系统，该方法主要包括：SYSLOG(网络事件日志协议)报文的发送者向 SYSLOG 报文的接收者发送安全传输升级指示信息；所述接收者接收到所述安全传输指示信息后，所述发送者、接收者在当前使用的传输层连接上建立安全传输连接，使用该安全传输连接在所述发送者、接收者之间传输 SYSLOG 报文。 利用本发明，可以使 Syslog 报文在安全传输和 TCP 传输之间自由转换，节约系统资源，同时为敏感信息提供安全保护。



1、一种传输网络事件日志协议报文的方法，其特征在于，包括步骤：

A、网络事件日志协议SYSLOG报文的发送者向SYSLOG报文的接收者发送安全传输指示信息；

B、所述接收者接收到所述安全传输指示信息后，所述发送者、接收者在当前使用的传输层连接上建立安全传输连接，使用该安全传输连接在所述发送者、接收者之间传输SYSLOG报文。

2、根据权利要求1所述的方法，其特征在于，所述的步骤A具体包括：

A1、在需要传输SYSLOG报文的发送者、接收者之间建立传输层连接，使用该传输层连接在所述发送者、接收者之间传输Syslog报文；

A2、当需要在所述发送者、接收者之间传输需要安全保护的Syslog报文时，所述发送者向所述接收者发送安全传输升级报文。

3、根据权利要求2所述的方法，其特征在于，所述的传输层连接包括：传输控制协议TCP连接。

4、根据权利要求2所述的方法，其特征在于，所述的安全传输升级报文包括：携带升级的指示信息的应用层报文。

5、根据权利要求2所述的方法，其特征在于，所述的安全传输升级报文包括：携带升级的指示信息的Syslog报文。

6、根据权利要求5所述的方法，其特征在于，包括：通过Syslog报文的设定字段或者结构化数据元素来携带所述升级的指示信息。

7、根据权利要求2、3、4、5或6所述的方法，其特征在于，所述的步骤B具体包括：

所述接收者接收到所述安全传输升级报文后，所述发送者、接收者基于所述传输层连接建立安全传输连接，然后，使用建立的安全传输连接在所述发送者、接收者之间传输Syslog报文。

8、根据权利要求7所述的方法，其特征在于，所述的步骤B还包括：

所述发送者发送所述安全传输升级报文后，当所述发送者、接收者之间

存在安全传输连接时，所述发送者直接使用该安全传输连接来向所述接收者发送SYSLOG报文。

9、根据权利要求7所述的方法，其特征在于，所述的步骤B还包括:

当所述需要安全保护的Syslog报文发送完毕后，SYSLOG报文的发送者向SYSLOG报文的接收者发送安全传输回退报文，然后，使用所述传输层连接在所述发送者、接收者之间传输SYSLOG报文。

10、根据权利要求9所述的方法，其特征在于，所述的步骤B还包括:

使用所述传输层连接在所述发送者、接收者之间传输SYSLOG报文后，关闭所述建立的安全传输连接。

11、根据权利要求9所述的方法，其特征在于，所述的安全传输回退报文包括：携带回退的指示信息的应用层报文。

12、根据权利要求9所述的方法，其特征在于，所述的安全传输回退报文包括：携带回退的指示信息的Syslog报文。

13、根据权利要求12所述的方法，其特征在于，包括：通过Syslog报文的设定字段或者结构化数据元素来携带所述回退的指示信息。

14、根据权利要求1所述的方法，其特征在于，所述的安全传输连接包括：传输层安全协议TLS连接或者块扩展交换协议BEEP连接或者安全外壳程序协议SSH连接。

15、一种传输网络事件日志协议报文的系统，包括Syslog报文的发送者、接收者，其特征在于，所述发送者、接收者包括：升级报文处理模块、和SYSLOG报文处理模块，其中，

升级报文处理模块：当需要在报文发送者和报文接收者之间传输需要安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送安全传输升级报文，向SYSLOG报文处理模块发送升级指示信息；报文接收者通过该模块接收到安全传输升级报文后，向SYSLOG报文处理模块发送升级指示信息;

SYSLOG报文处理模块：通过该模块使用传输层传输连接或安全传输连接在报文发送者和报文接收者之间传输Syslog报文，根据升级报文处理模块传递过来的升级指示信息从传输层传输连接升级到安全传输连接。

16、根据权利要求15所述的系统，其特征在于，所述的SYSLOG报文处

理模块包括:

安全传输模块：当接收到升级报文处理模块传递过来的升级指示信息后，基于所述发送者、接收者之间当前使用的传输层连接建立安全传输连接，使用该安全传输连接在所述发送者和报文接收者之间传输SYSLOG报文。

17、根据权利要求15所述的系统，其特征在于，包括:

回退报文处理模块：当需要在报文发送者和报文接收者之间传输不需要进行安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送安全传输回退报文，向SYSLOG报文处理模块发送回退指示信息；报文接收者通过该模块接收到安全传输回退报文后，向SYSLOG报文处理模块发送回退指示信息。

18、根据权利要求17所述的系统，其特征在于，所述的SYSLOG报文处理模块包括:

传输层传输模块：当接收到回退报文处理模块传递过来的回退指示信息后，或者根据预定设置，使用传输层传输连接在所述发送者和报文接收者之间传输SYSLOG报文。

传输网络事件日志协议报文的方法和系统

技术领域

本发明涉及网络通讯领域，尤其涉及一种传输网络事件日志协议报文的方法和系统。

背景技术

SYSLOG（网络事件日志协议）是在各种网络操作系统中广泛应用的事件通告传递协议，当前一些主要的操作系统，如微软Windows、各种Unix以及Linux都实现了SYSLOG协议。IETF（因特网工程部）也在致力于SYSLOG协议的标准化，统一各种SYSLOG的报文格式定义。

SYSLOG协议采用Client/Server（客户端/服务器）模式的通信方式，Client是事件报文的发送者，Server是事件报文的接收者。Client可以是事件的产生者，比如一个设备或进程，也可能是一个中继实体，中继实体对从其它发送者（事件产生者或其他中继实体）收到的SYSLOG事件进行处理后发给其它的接收者。

SYSLOG协议是单向的通信协议，事件报文只从发送者发送到接收者，接收者不发送任何确认报文、连接启动和连接关闭等报文，也就是说接收者在SYSLOG协议层次总是不发送任何报文给发送者（但是下层的传输协议可能需要双向通信）。

SYSLOG协议是一个基于文本的协议，所有的参数名称和参数值都是采用文本，并且避免使用ASCII编码中编码值低于32的字符，即避免使用控制字符，从下层传输协议的角度来看，可以将Syslog报文简单地理解为一个文本块。

Syslog协议报文的格式如下：

1、每个报文由三个部分组成：报文头、结构化数据和MSG（消息）部

分。

2、上述报文头是一个由打印字符构成的串，由如下的几个部分组成，各个部分之间由空格分开，上述几个部分分别为：

PRI，优先级；

VERSION，Syslog协议版本号；

TIMESTAMP，时标；

HOSTNAME，主机名；

APP-NAME，应用名；

PROCID，进程ID；

MSGID，报文ID。

3、上述结构数据是由一系列结构化元素构成，每个结构化元素由结构化元素名称以及一系列的参数名和参数值对组成

4、上述MSG是由可打印字符构成的消息，一般为事件描述信息。

目前基本上采用UDP（用户数据报协议）进行SYSLOG报文的传输，根据SYSLOG报文长度和UDP报文长度的关系，在采用UDP进行SYSLOG报文的传输时，每个UDP报文只能传输一个SYSLOG报文。采用UDP来传递SYSLOG报文的协议层次示意图如图1所示的SYSLOG协议的协议栈结构的A部分。

UDP虽然具有简单灵活的特点，但是UDP是一个不可靠的无连接协议，在采用UDP的报文传送过程中可能丢失报文，而SYSLOG报文也不处理丢包等情况，因此，采用UDP来传递SYSLOG报文可能造成传递的事件信息丢失。TCP（传输控制协议）是可靠的面向连接的协议，为了改善数据传输的可靠性，可以采用TCP来传输SYSLOG报文。采用TCP来传递SYSLOG报文的协议层次示意图如图1所示的SYSLOG协议的协议栈结构的B部分。

目前，Internet网络安全问题越来越成为网络稳定运行的关键问题，同样syslog协议也存在着如下的安全风险：

1、信息篡改，SYSLOG报文在传输的过程中被中间的恶意网络节点非法篡改。

2、信息泄露，SYSLOG报文在传输过程中被非法拦截，并获取了SYSLOG报文中的信息，如事件的描述信息。

3、身份仿冒，一个恶意节点仿冒一个合法节点参与到SYSLOG的通信中。

因此，为了解决SYSLOG报文的安全问题，可以将SYSLOG报文传输在某些安全协议上，比如TLS（传输层安全协议）、BEEP（块扩展交换协议）和SSH（安全外壳程序协议），这些安全协议能够提供保密性、完整性和数据源验证等安全机制，这样就能够解决SYSLOG报文的安全问题。采用TCP和安全协议来传递SYSLOG报文的协议层次示意图如图1所示的SYSLOG协议的协议栈结构的C部分。

现有技术中一种使用TLS传输Syslog报文的方法为：采用TLS的缺省使用方式。当syslog向一个特定的TCP端口发起请求，则认为该TCP连接上的所有的Syslog数据需要使用TLS实现保护。因此，在TCP连接建立后，则直接开始TLS握手的过程，握手过程完成后在TLS上传输Syslog报文。该TCP连接上的所有Syslog报文都使用TLS来传输，直到通信结束。

目前，很多设备或日志服务器实现了TCP传输和安全传输，但在实际应用中，一些设备或日志服务器并不希望对于所有的Syslog报文都使用安全传输，只希望对于一些特定Syslog报文使用安全传输，在这些特定Syslog报文发送结束后再回退到原来的TCP连接上，使用TCP连接来传输Syslog报文，不再使用安全传输。

现有技术中一种使用TCP和TLS来交替传输Syslog报文的方法为：采用重新建立连接的方式。具体处理过程如下：

1、首先建立一个TCP连接，通过该TCP连接来传输Syslog报文。

2、当需要传输敏感的Syslog报文时，将上述TCP连接关闭，然后。新创建一个TCP/TLS连接，通过该TCP/TLS连接来传输上述敏感的Syslog报文。

3、当上述敏感的Syslog报文传输结束后，关闭上述TCP/TLS连接，然后，再新建立一个TCP连接，并通过该TCP连接上继续传输Syslog报文。

上述现有技术中使用TCP和TLS来交替传输Syslog报文的方法的缺点为：需要多次创建和关闭连接，从而浪费系统资源。

发明内容

本发明的目的是提供一种传输网络事件日志协议报文的方法和系统，从而可以使Syslog报文在安全传输和TCP传输之间自由转换，节约系统资源。

本发明的目的是通过以下技术方案实现的:

一种传输网络事件日志协议报文的方法，包括步骤:

A、网络事件日志协议SYSLOG报文的发送者向SYSLOG报文的接收者发送安全传输指示信息;

B、所述接收者接收到所述安全传输指示信息后，所述发送者、接收者在当前使用的传输层连接上建立安全传输连接，使用该安全传输连接在所述发送者、接收者之间传输SYSLOG报文。

所述的步骤A具体包括:

A1、在需要传输SYSLOG报文的发送者、接收者之间建立传输层连接，使用该传输层连接在所述发送者、接收者之间传输Syslog报文;

A2、当需要在所述发送者、接收者之间传输需要安全保护的Syslog报文时，所述发送者向所述接收者发送安全传输升级报文。

所述的传输层连接包括：传输控制协议TCP连接。

所述的安全传输升级报文包括：携带升级的指示信息的应用层报文。

所述的安全传输升级报文包括：携带升级的指示信息的Syslog报文。

通过Syslog报文的设定字段或者结构化数据元素来携带所述升级的指示信息。

所述的步骤B具体包括:

所述接收者接收到所述安全传输升级报文后，所述发送者、接收者基于所述传输层连接建立安全传输连接，然后，使用建立的安全传输连接在所述发送者、接收者之间传输Syslog报文。

所述的步骤B还包括:

所述发送者发送所述安全传输升级报文后，当所述发送者、接收者之间

存在安全传输连接时，所述发送者直接使用该安全传输连接来向所述接收者发送SYSLOG报文。

所述的步骤B还包括:

当所述需要安全保护的Syslog报文发送完毕后，SYSLOG报文的发送者向SYSLOG报文的接收者发送安全传输回退报文，然后，使用所述传输层连接在所述发送者、接收者之间传输SYSLOG报文。

所述的步骤B还包括:

使用所述传输层连接在所述发送者、接收者之间传输SYSLOG报文后，关闭所述建立的安全传输连接。

所述的安全传输回退报文包括：携带回退的指示信息的应用层报文。

所述的安全传输回退报文包括：携带回退的指示信息的Syslog报文。

通过Syslog报文的设定字段或者结构化数据元素来携带所述回退的指示信息。

所述的安全传输连接包括：传输层安全协议TLS连接或者块扩展交换协议BEEP连接或者安全外壳程序协议SSH连接。

一种传输网络事件日志协议报文的系统，包括Syslog报文的发送者、接收者，所述发送者、接收者包括：升级报文处理模块、和SYSLOG报文处理模块，其中，

升级报文处理模块：当需要在报文发送者和报文接收者之间传输需要安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送安全传输升级报文，向SYSLOG报文处理模块发送升级指示信息；报文接收者通过该模块接收到安全传输升级报文后，向SYSLOG报文处理模块发送升级指示信息;

SYSLOG报文处理模块：通过该模块使用传输层传输连接或安全传输连接在报文发送者和报文接收者之间传输Syslog报文，根据升级报文处理模块传递过来的升级指示信息从传输层传输连接升级到安全传输连接。

所述的SYSLOG报文处理模块包括:

安全传输模块：当接收到升级报文处理模块传递过来的升级指示信息

后，基于所述发送者、接收者之间当前使用的传输层连接建立安全传输连接，使用该安全传输连接在所述发送者和报文接收者之间传输SYSLOG报文。

包括:

回退报文处理模块：当需要在报文发送者和报文接收者之间传输不需要进行安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送安全传输回退报文，向SYSLOG报文处理模块发送回退指示信息；报文接收者通过该模块接收到安全传输回退报文后，向SYSLOG报文处理模块发送回退指示信息。

所述的SYSLOG报文处理模块包括:

传输层传输模块：当接收到回退报文处理模块传递过来的回退指示信息后，或者根据预定设置，使用传输层传输连接在所述发送者和报文接收者之间传输SYSLOG报文。

本发明通过在报文发送者和报文接收者之间传递升级或回退报文，在使用安全传输连接（比如TLS连接）来传递SYSLOG报文的时候，并不关闭以前建立的TCP连接。从而可以使Syslog报文在安全传输和TCP传输之间自由转换。在执行从安全传输回退到TCP传输时，可以重用以前建立的TCP连接，不需要重复地建立TCP连接，从而可以节约系统资源，同时为敏感信息提供安全保护。

附图说明

图1为SYSLOG协议的协议栈结构示意图;

图2为本发明所述方法的实施例的处理流程图;

图3为本发明所述TCP/TLS升级和回退过程的示意图;

图4为本发明所述系统的实施例的结构示意图。

具体实施方式

本发明提供了一种传输网络事件日志协议报文的方法和系统，本发明的核心为：报文发送者和报文接收者之间通过传递升级或回退报文来执行从

TCP升级到TLS或从TLS回退到TCP的过程，在使用TLS来传递SYSLOG报文的时候，并不关闭以前建立的TCP连接。

下面结合附图来详细描述本发明，本发明所述方法的实施例的处理流程如图2所示，包括如下步骤:

步骤2-1、使用TCP连接来传输普通SYSLOG报文。

首先在需要传输SYSLOG报文的报文发送者和报文接收者之间建立一个传输层连接，比如，TCP连接。根据预定设置，通过该TCP连接在报文发送者和报文接收者之间之间传输一些不需要进行安全保护的Syslog报文，即Syslog报文直接在TCP协议上传输。

步骤2-2、通过传递安全传输升级报文在报文发送者和报文接收者之间之间建立TLS连接，使用TLS连接来传输需要安全保护的SYSLOG报文。

当需要在上述报文发送者和报文接收者之间传输一些敏感的、需要安全保护的Syslog报文时，报文发送者向报文接收者发送一个安全传输升级报文。

上述安全传输升级报文可能的构成方式包括:

1，一个特殊的应用层报文，该报文不采用Syslog的报文格式，携带升级的指示信息。当报文接收者接收到这个Syslog报文后，则开始执行升级功能。

2，一个特殊的Syslog报文，该报文使用Syslog的报文格式，但是其中特定的字段能够指出该报文是用来实现升级。

比如，可以在上述特殊的Syslog报文的报文头部分使用一些特别的值，比如在PRI（基群速率接口）字段中设置特别的值，该特殊的值用来实现升级功能。当报文接收者发现收到的Syslog报文的PRI字段的值为上述特别的值时，则开始执行升级功能。

3、一个特殊的Syslog报文，在该Syslog报文的结构化数据部分使用一些特别的结构化数据元素，该结构化数据元素的标识或构成该结构化元素的参数名/参数值对用来实现升级的指示信息，当报文接收者发现收到的Syslog报文的结构化数据部分包含上述标识或参数名/参数值时，则开始执行升级功能。

4、一个普通的syslog报文，在传输一般的事件信息的同时，在该Syslog报文的结构化数据部分使用一些特别的结构化数据元素，该结构化数据元素的标识或构成该结构化元素的参数名/参数值对用来实现升级的指示信息，当报文接收者发现收到的Syslog报文的结构化数据部分包含上述标识或参数名/参数值时，则开始执行升级功能。

当报文接收者接收到上述安全传输升级报文后，则立即基于上述TCP连接和报文发送者开始进行TLS握手的过程，TLS握手的过程完成后，在报文接收者、报文发送者之间将建立一个基于上述TCP连接的TLS连接。如果在报文接收者、报文发送者已经存在一个TLS连接，就不进行该TLS握手过程。

上述TLS为一种基于有连接的可靠传输的安全协议，能够为上层协议提供验证、完整性检查、数据保密性和防回放等安全服务，在网络访问中广泛使用，在实际应用中还可以采用其它安全协议，比如，BEEP或者SSH。

在上述TLS连接建立后，后续的敏感的Syslog报文就使用该TLS连接进行传输。在使用该TLS来传输Syslog报文时，不关闭上述已经建立的TCP连接。

步骤2-3、通过传递安全传输回退报文，重新使用TCP连接来传输普通SYSLOG报文。

在上述敏感的、需要进行安全保护的Syslog报文传输完毕后，上述报文发送者向报文接收者发送一个安全传输回退报文。

上述安全传输回退报文可能的构成方式包括:

1，一个特殊的应用层报文，该报文不采用Syslog的报文格式，携带回退的指示信息。当报文接收者接收到这个Syslog报文后，则开始执行回退功能。

2，一个特殊的Syslog报文，该报文使用Syslog的报文格式，但是其中特定的字段能够指出该报文是用来实现回退。

比如，可以在上述特殊的Syslog报文的报文头部分使用一些特别的值，比如在PRI（基群速率接口）字段中设置特别的值，该特殊的值用来实现回退的指示信息。当报文接收者发现收到的Syslog报文的PRI字段的值为上述

特别的值时，则开始执行回退功能。

3、一个特殊的Syslog报文，在该Syslog报文的结构化数据部分使用一些特别的结构化数据元素，该结构化数据元素的标识或构成该结构化元素的参数名/参数值对用来实现回退的指示信息，当报文接收者发现收到的Syslog报文的结构化数据部分包含上述标识或参数名/参数值时，则开始执行回退功能。

4、一个普通的syslog报文，在传输一般的事件信息的同时，在该Syslog报文的结构化数据部分使用一些特别的结构化数据元素，该结构化数据元素的标识或构成该结构化元素的参数名/参数值对用来实现回退的指示信息，当报文接收者发现收到的Syslog报文的结构化数据部分包含上述标识或参数名/参数值时，则开始执行回退功能。

当报文发送者发送了上述安全传输回退报文后，后续Syslog报文将重新使用上述TCP连接来传输，此时，可以根据实际需要关闭或不关闭上述TLS连接。

上述TCP/TLS升级和回退过程的示意图如图3所示。

本发明所述系统的实施例的结构示意图如图4所示。包括报文发送者和报文接收者。报文发送者和报文接收者中包括如下的模块：

升级报文处理模块：当需要在报文发送者和报文接收者之间传输一些敏感的、需要安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送一个上述安全传输升级报文，并且向其内部SYSLOG报文处理模块发送升级指示信息；报文接收者通过该模块接收到上述安全传输升级报文后，向其内部SYSLOG报文处理模块发送升级指示信息。

回退报文处理模块：当需要在报文发送者和报文接收者之间传输一些不需要安全保护的Syslog报文时，报文发送者通过该模块向报文接收者发送一个上述安全传输回退报文，并且向其内部SYSLOG报文处理模块发送回退指示信息；报文接收者通过该模块接收到上述安全传输回退报文后，向其内部SYSLOG报文处理模块发送回退指示信息。

SYSLOG报文处理模块：通过该模块使用传输层连接或安全传输连接（比如TLS连接）在报文发送者和报文接收者之间传输Syslog报文，根据升

级报文处理模块和回退报文处理模块发送的升级指示信息和回退指示信息，进行相应的从TCP升级到TLS或从TLS回退到TCP的操作。SYSLOG报文处理模块包括：传输层传输模块、安全传输模块。

其中，传输层传输模块：当接收到回退报文处理模块发送的回退指示信息后，或者根据预定设置，使用传输层连接在报文发送者和报文接收者之间传输SYSLOG报文。

其中，安全传输模块：当接收到升级报文处理模块发送的升级指示信息后，基于所述发送者、接收者之间当前使用的传输层连接建立安全传输连接，使用该安全传输连接在报文发送者和报文接收者之间传输SYSLOG报文。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

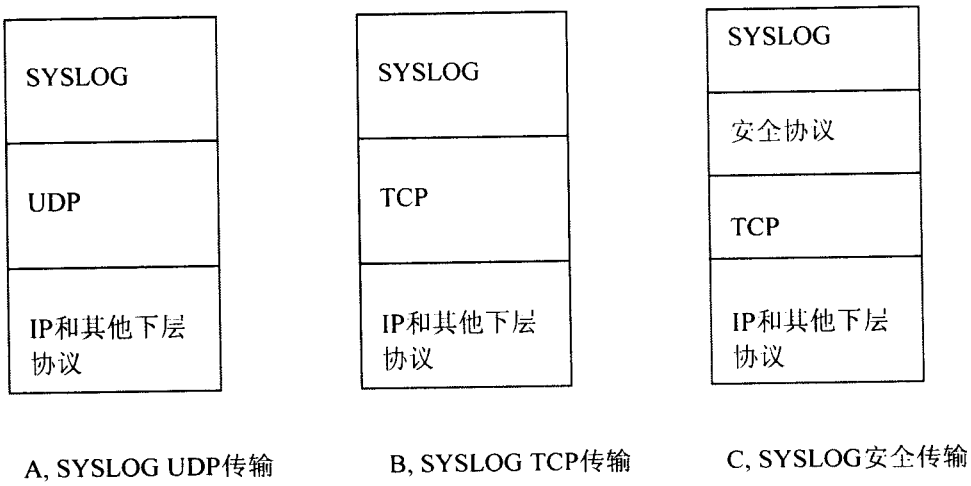

SYSLOG
UDP
IP和其他下层协议
SYSLOG
TCP
IP和其他下层协议
SYSLOG
安全协议
TCP
IP和其他下层协议
A, SYSLOG UDP传输
B, SYSLOG TCP传输
C, SYSLOG安全传输

图1

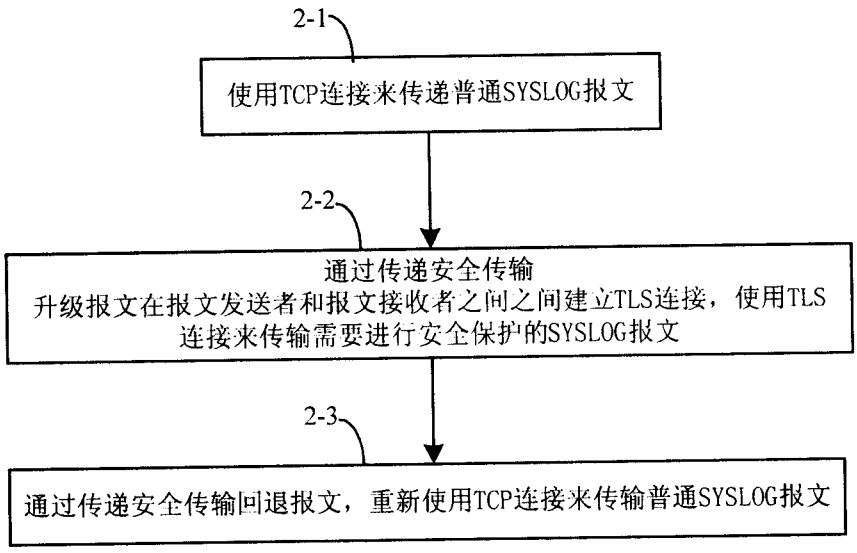

2-1
使用TCP连接来传递普通SYSLOG报文
2-2
通过传递安全传输
升级报文在报文发送者和报文接收者之间之间建立TLS连接，使用TLS连接来传输需要进行安全保护的SYSLOG报文
2-3
通过传递安全传输回退报文，重新使用TCP连接来传输普通SYSLOG报文

图2

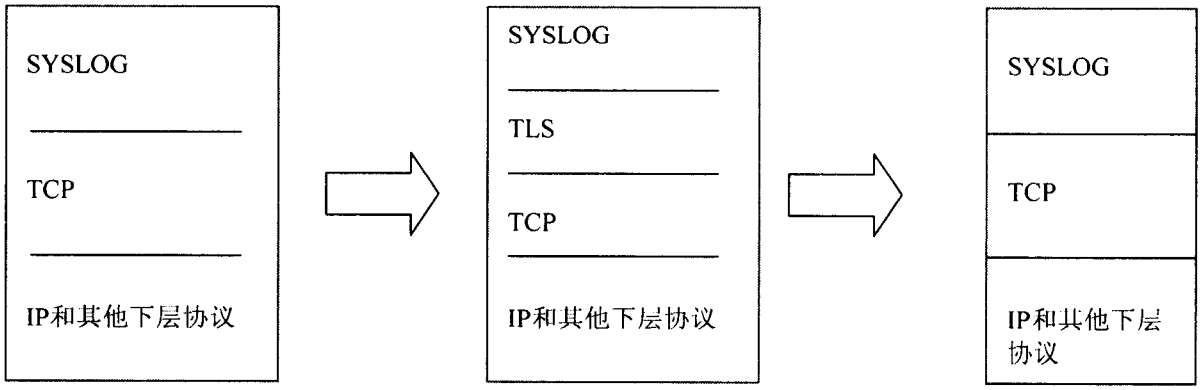

SYSLOG
TCP
IP和其他下层协议
SYSLOG
TLS
TCP
IP和其他下层协议
SYSLOG
TCP
IP和其他下层协议
SYSLOG TCP传输
SYSLOG TLS传输
SYSLOG TCP传输

图3

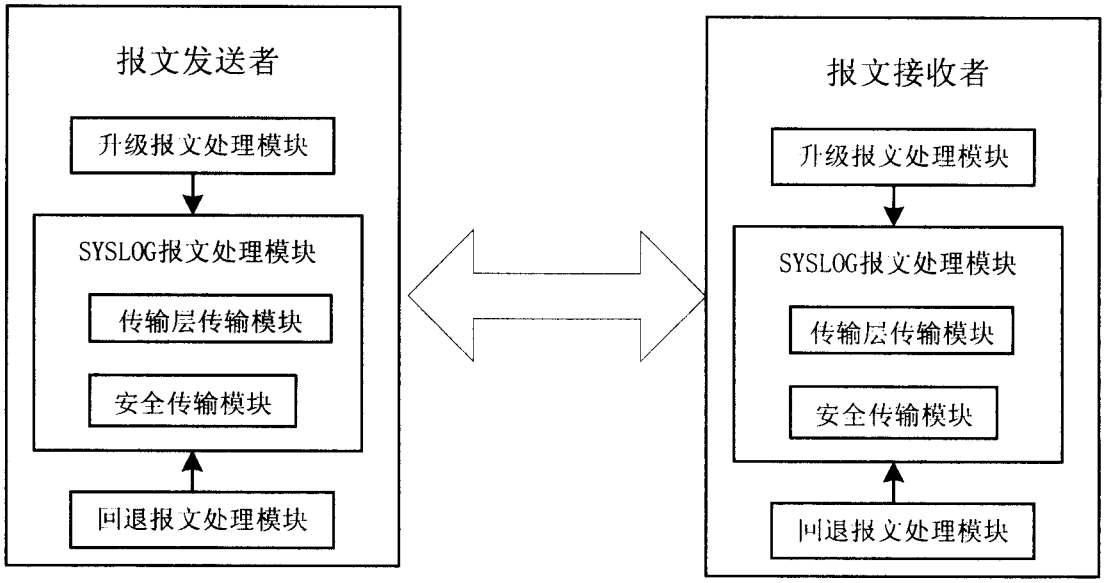

报文发送者
升级报文处理模块
SYSLOG报文处理模块
传输层传输模块
安全传输模块
回退报文处理模块
报文接收者
升级报文处理模块
SYSLOG报文处理模块
传输层传输模块
安全传输模块
回退报文处理模块

图4